FEDERAL REPUBLIC OF GERMANY

Patent Application
DE 100 59 230 A 1

Int. Cl. [7]: H 04 L 9/32

File Number: 100 59 230.9
Filing Date: 29 November 2000
Laid Open: 13 June 2002

GERMAN PATENT AND TRADEMARK OFFICE

Applicant:
4FriendsOnly.com Internet Technologies AG, 98693 Ilmenau, DE

Representative:
Engel und Kollegen, 98527 Suhl

Inventor:
Nützel, Jürgen, Dr.-Ing., 98693 Ilmenau, DE; Böhme, Thomas, Dr.rer.nat. habil., 98693 Ilmenau, DE; Stein, Mathias, 87629 Füssen, DE; Schwetschke, Stefan, 87663 Lengenwang, DE

Citations:

DE	199 06 450 C1
DE	199 06 449 C1
DE	198 48 492 A1
EP	4 38 154 B1
EP	10 45 386 A1
WO 2	000 64 111 A1
WO 2	000 27 067 A1
WO	99 67 917 A1
JP	10-1 77 523 A1

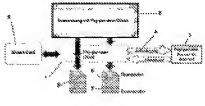
CHENG, H. et al.: Partial encryption of compressed images and videos. In: IEEE Transactions on Signal Processing, Vol. 48, No. 8, 8 August 2000, pp. 2439-2451;

The following specifications are taken from the documents submitted by the applicant

Request for examination pursuant to § 44 PatG submitted

Method for making available multimedia data quantities and data processing system

The invention relates to a method for making available multimedia data quantities to a user. The method comprises the following steps: providing an essence file (7) on a remote server (3), which comprises at least a portion of the multimedia data quantity; encryption of the essence file; transmission of the encrypted essence file to a local computer (1) to which the user has access; storage of the encrypted essence file on a local data medium of the local computer; decryption of the essence file during the execution of a data processing program (2) on the local computer; reproduction of the multimedia data quantity via an output apparatus during the execution of the data processing program on the local computer. Herein preferably a division of the multimedia data quantity takes place into a basic file (6) and an essence file (7) according to a predetermined division algorithm, and a linkage of the basic file and of the essence file to the multimedia data quantity during the execution of the data processing program (2) on the local computer. The invention also relates to a data processing system for making available multimedia data quantities.



Description

[0001] The present invention relates to a method for making available multimedia data quantities to one or any number of users. The invention furthermore relates to a data processing system which comprises a server, a local computer and a data transmission connection between the server and the computer and is suitable for making available multimedia data quantities. In the broader sense, making available should be understood providing the data as well as also the authorization of the users for using these data.

[0002] Various methods are known to multiply electronic data and for distributing the produced copies to different users. Software producers are interested in preventing the free copying of certain data in order to ensure thereby that investment intensive software can be sold in sufficient quantity. Although the unauthorized copying of electronic data is at least partially forbidden by copyright regulations, the unauthorized multiplication of data processing programs (application software) and also of multimedia data of diverse type can hardly be controlled. One feasibility for the partial restriction of unauthorized multiplication of such data consists therein that during the installation process of a software a data key is called up which is entered manually by the user as a character sequence and subsequently permits utilization of the software. It is understood, that therewith cannot be prevented that the key, most often handed to the user in the form of print, is passed on with the copied data.

[0003] In various areas of application programs, for example with computer games, there is in addition the requirement of the software producers to provide and make known the software as fast as possible to a broad public in order to increase thereby the quantity and rate of distribution. For this purpose, executable versions of the software, time and/or functionally limited, are distributed to potential customers free of charge or at a very low price. After the user has been able to test at least partially this software, there is the possibility of purchasing commercially a complete version of the software. The electronic distribution of the restricted versions and of the full version of the software, however, presents difficulties, at least if fairly large data quantities must be transferred to the user. When providing the data quantities on permanent data media (for example CD ROM), a method was utilized at times, in which to the user, after payment of the

demanded purchase price, only an enable key is transmitted which subsequently permits access to all data stored previously on the data medium. Herein, however, there is the risk that the enable key can also readily be applied to produced copies of the data.

[0004] One problem addressed by the present invention, consequently, comprises providing a method for making available, in particular, multimedia data quantities through which it becomes possible to transmit to a user, if indicated, in several partial steps, portions of a multimedia data quantity, wherein the uncontrolled multiplication of at least essential parts of this data quantity is to be prevented, wherein the possibility is given of transmitting to the user certain parts of the data quantity only against payment of a purchasing price, and wherein the data subquantity provided against remuneration is also to be suitable with respect to its size of being transmitted across online connections.

[0005] These and additional problems are resolved through the method according to the invention, which comprises the following steps:

- providing an essence file on a remote server, which file comprises at least a portion of the multimedia data quantity;
- encrypting the essence file;
- transmitting the encrypted essence file to a local computer to which the user has access;
- storing the encrypted essence file on a local data medium of the local computer;
- decrypting the essence file during the execution of a data processing program on the local computer;
- reproducing the multimedia data quantity via an output apparatus during the execution of the data processing program on the local computer.

[0006] This method permits generally to make multimedia data available to any number of users, wherein, on the one hand, the user authorized to access the data can be selected according to certain criteria (for example payment of remuneration, registration or the like) and, on the other hand, unhindered multiplication and distribution of the data can be reliably prevented. The method can be applied wherever multimedia data are significant components of software applications. A significant difference to, for example, conventional methods in which only the

enabling of data already transferred to the potential user, is that the user here lacks the multimedia data or at least essential portions of these data such that even with the knowledge of an enable key, the software applications cannot be operated or only with considerable restrictions as long as the required data cannot be obtained from an authorized distributor.

[0007] According to an especially appropriate embodiment, the method comprises furthermore the following steps:

- division of the multimedia data quantity into a basic file and an essence file, according to a predetermined division algorithm.
- transmission of the basic file and of the esssence file;
- storage of the basic file and of the encrypted essence file on a local data medium of a local computer;
- linkage of the basic file and of the essence file to form the multimedia data quantity during the execution of the data processing program on the local computer, after the decryption of the essence file.

[0008] This variant of the method permits splitting one or several files of the multimedia data quantity into two files each, a so-called basic file and one (or several) so-called essence files. In contrast to the above described embodiment, the user with the basic file has already portions of the multimedia data quantity, which, however, are only usable in the presence of the essence file or at least only become fully usable (for example with respect to quality and function). The subfiles, which in this case are parts of a total file (the multimedia data quantity) can be distributed in various data transmission channels to interested users. It is herein advantageous that the basic file can be significantly greater than the essence file such that the basic file, for example, can be transferred to the user on a permanent and cost-effective data medium, for example a CD ROM. With respect to the data content, the essence file is so selected that, while in most cases it is markedly smaller than the basic file, it does, however, contain essential information which is of decisive significance for a qualitative and/or complete reproduction of the multimedia data quantity. The essence file can preferably be transmitted to the user upon separate request by the user. It is therewith possible to supply directly and upon request to the

recipient any number of essence files, if appropriate, against the paid remuneration. .

[0009] The encryption of the essence file entails, moreover, the advantage that the transfer of the encrypted essence file to unauthorized users will not take place since these [users] are not able to decrypt the essence file without knowning the private key of the authorized user.

[0010] The invention, furthermore, provides a data processing system of the above described type, which further comprises:

- an encryption unit which encrypts an essence file which includes at least a portion of the multimedia data quantity;
- an archive generating unit of the server, which combines the encrypted essence file with user-specific data to form a transfer archive and makes this available for the online transmission via the data transmission connection;
- an updating unit of the local computer, which carries out entries into a system registration data base of the local computer, which specify the contents of the transmitted transfer archive;
- a decryption unit of the local computer which, during the execution of a data processing program, decrypts the essence file;
- an output unit which outputs the multimedia data quantity to the output apparatus.

[0011] Said units of the data processing systems are preferably realized by suitable software routines such that, with respect to their technical apparatus characteristics or their hardware, conventional computers can be utilized.

[0012] The invention also provides suitably configured computers which can assume the tasks of the server or of the local computer in order to perform jointly the steps of the method according to the invention.

[0013] According to an appropriate embodiment of the method, the encryption of the essence file takes place in a first step (upon request, when archive is established) with the application of a symmetric encryption algorithm. The encryption is preferably only carried out when the essence file is requested by a user, wherein during each session/request a session-specific key is generated (session key). Each user receives the essence file encrypted using a different key. The session-specific key required for this purpose, which, if necessary, is "determined by throwing

dice" as a random number, is encrypted in a second step in an asymmetric encryption algorithm, wherein the public key is utilized of the user who has requested the transmission of the essence file.

[0014] According to an especially preferred embodiment, the session key encrypted using the public key of the user can additionally be encrypted symmetrically with a user-specific key (password). Therewith the identification of the user can also be ensured in cases in which the user is not equipped with a smart card. The password can be transmitted to the user, for example via e-mail, wherein the e-mail address of the user is checked.

[0015] Since the encryption of the essence file only takes place during the execution of the data processing program on the local computer, storage of the essence file in the unencrypted state on the local computer is not required at any time. For an unauthorized third party, access to the encrypted essence file is thus useless since he does not know the private key of the authorized user necessary for the decryption of the essence file.

[0016] According to an advantageous embodiment of the data processing system provided by the invention, the private key of the recipient is stored on a smart card, from which this private key cannot be read out. In the decryption of the essence file or of the symmetric key, the data processing program accesses the smart card in order to carry out the asymmetric decryption of the symmetric session-specific key (session key). In the event that the private key was additionally encrypted using a password, the decryption with the password must first take place.

[0017] According to a preferred embodiment of the method, a transfer archive is generated on the server, which archive comprises the encrypted essence file, a server signature, a check section, a data identification section and a user data section. The server signature allows the recipient to check the identity of the server in order to prevent that unauthorized third parties take over the functions of the server and therein accept, for example, unauthorized payments from the recipient. The data identification section contains *inter alia* all specifications necessary for combining the basic file and the essence file. It is, for example, possible that in the transfer archive a reference to an algorithm is contained, which is already available at the user/recipient as part of the data processing program and which makes possible the correct combination of basic file and essence file. However, it is also conceivable that the transfer archive itself contains

the required algorithm for the combination of these files.

[0018] The user data section of the transfer archive permits the identification of the user/recipient. Corresponding data are, if necessary, stored on servers in a special data base. In this manner it is possible to trace each at a later point in time which user has received which transfer archive and therewith which essence file. This information is required in order to be able to carry out the correct billing if the essence file is sent to the recipient against payment. In addition, already completed transmissions can be repeated if such is necessary due to transmission interferences or other data losses.

[0019] Handling of the encrypted essence file transmitted to the local computer is simplified in that in a system registration data base of the local computer corresponding entries are generated. From such entries can be determined the data processing program in progress, the storage location of the transfer archive as well as the essence files contained therein in order to access these. The system registration data base contains therewith specification regarding which essence files are available on the local computer and in which transfer archive they are stored. In the absence of essence files, an online connection to the server can be established in order to allow the necessary essence file to be transmitted.

[0020] Further advantages, details and further developments are evident in the following description of preferred embodiments of the invention with reference to the drawing. Therein depict:

[0021] Fig. 1 a block diagram of a data processing system according to the invention;

[0022] Fig. 2 a fundamental depiction of the combination of a basic file and of an essence file to form a multimedia data quantity;

[0023] Fig. 3 a flow chart which indicates the most important method step in the request and transmission of an essence file;

[0024] Fig. 4 the general structure of a form page which is utilized during the request of an essence file;

[0025] Fig. 5 the general structure of a transfer archive.

[0026] Figure 1 shows in a block diagram the general structure of a data processing system according to the invention. This system will be denoted in the following as a pay-per-use

application. Pay-per-use is to be understood herein as a stepwise sale of a multimedia data quantity.

[0027] On a local computer 1 a data processing program 2 (application software) is executed, in the depicted example a PC game, whereby the local computer is configured as client. There is furthermore a server 3 which preferably is structured as an Internet server and which can be accessed by the local computer 1 via a temporary online connection 4. Via the online connection 4 a data request is transmitted from the local computer to the server as well as also a so-called download is carried out, i.e. a data transmission from the server to the local computer.

[0028] During the execution of the data processing program 2, the local computer 1 accesses a basic file 6. The basic file in this case is already available on a permanent data medium. For example, the user receives a CD ROM, which, *inter alia*, comprises the basic file 6 and is provided to the local computer. The basic file 6 is a subfile out of a multimedia data quantity which initially is only incompletely available to the local computer. The difference between the multimedia data quantity and the basic file 6 is an essence file 7, which is also required for the complete execution of the data processing program 2. The essence file 7 is ready on the server 3 and can be understood as a supplement of the basic file (plugin). In the event of appropriate authorization, the essence file 7 is downloaded from the sever 3. However, before the transmission an encryption of the essence file 7 takes place. The details of the dissembling of the multimedia data quantity into the basic file and the essence file as well as the feasibilities of obtaining and storing the essence file will be explained below.

[0029] In a modified embodiment the multimedia data quantity required by the application program is not comprised of subfiles but rather is represented in a complete essence file 8, i.e. there is no basic file. It is therewith possible, for example, to make available functional expansions for the application program, which at the time of the delivery of the application program to the user, were potentially not available. The complete essence file 8 could, for example, contain a new level of a PC game for which there is not yet a basic file at the applicant.

[0030] The embodiment depicted in Fig. 1 comprises furthermore a smart card unit 9 which serves for the encryption or decryption of data. The smart card unit is capable of cooperating with a smart card on which a private key of the user/recipient is stored. In other embodiments

the smart card unit 9 can be replaced by a "virtual smart card", i.e. the private key is stored on a local data medium of the local computer 1 or is concealed in a special manner (for example encrypted with hardware parameters). The details of encryption or decryption of data, to the extent they are not already known to the person of skill in the art, will also be discussed in detail below.

[0031] In order to be able to utilize the principle applied here of data distribution, transmission and composition for several data processing programs, through suitable software routines on the local computer 1 a pay-per-use client is imaged. The pay-per-use client can be, for example, a dynamically loadable program library (DLL). It is herein sufficient if the programming interface (API) of the client is revealed in order for several application programs to be able to access this interface. Revealing the source code of the pay-per-use client is not required, which is also desirable for reasons of security.

[0032] The data processing program (application software) can, for example, be realized as a Windows application and use the programming feasibilites customary under this operating system. The operating system should at least be capable of carrying out the management of files, i.e. basic file and essence file, that means, a suitable file system must be available. This self-management includes the capability of reading files from a data medium (for example hard drive) and to transmit them for processing to the main drive.

[0033] The goal of the division of multimedia data quantities into at least one basic file and at least one essence file consist primarily in transferring the generated subfiles over different distribution channels to potential user/recipients. In general, division of a data quantity is also possible in other data forms, however, the removal of a certain fraction of data from an executable file (application program) would not be very meaningful if the goal is that the remaining basic file, for example for purposes of demonstration, continues to be executable. However, if in the execution of a data processing program multimedia data quantities are required, cutting out a certain fraction of these data quantities can take place such that the data processing program remains executable even if with restricted quality or decreased function extent. As was already explained above, multimedia data quantities can also be provided which are not split. The division of the data quantity is especially of interest in multimedia files, since,

for example video and audio data, also lead to relatively large files even when compression methods are applied, which files can no longer be transmitted, for example, via online connections or only at high cost and time expenditures. The division of the data quantity utilized here is in so far especially suitable for multimedia data. The goal herein is that the basic file with respect to its quality and/or its breadth of function is so far restricted that a meaningful and high quality utilization is no longer possible. Therefore, as a function of the type of data, from the total quantity of the multimedia data those data must be shifted into one or several essence files which effect such quality or function loss. On the other hand, there is the demand of keeping the essence file as small as possible in order to permit in particular an online transmission of the essence file. In the following, examples will be described which illustrate clearly the division into the basic file and the essence file for special data formats.

[0034] In computer games, but also in CAD and other planning applications, images or three-dimensional models are frequently utilized in order to display certain scenarios on the picture screen. These multimedia data are each required completely by the application software in order to generate an exact graphic display. In files, which contain such data, frequently at the file start (header) necessary information for the interpretation of the succeeding data are stored (for example GIF files). If this file header is removed, necessary data are lacking for displaying correctly the remaining data contained in this file. For example, in a color GIF graphic the color table (3 x 256 bytes) can be removed whereby the entire file becomes largely unusable. The desired division of the multimedia data quantity in such data formats is thus going to be such that the basic file contains the major portion of the data quantity while the essence file comprises only the file header or certain information from the file header.

[0035] Other data are of a data type that can be referred to as "dynamic". These are for example video or audio files, wherein the concatenated files have a relationship to one another that is defined in time. In the case of these file types it would be sensible to cut out only a few starting values of the files, since subsequently all data, later in time, can be reproduced undisturbed. It is rather required to split the multimedia data quantity continuously in time such that essential portions of the data can be transferred into the essence file over the entire time period of the reproduction of the total data quantity. The multimedia data quantity in this case is

reproduced continuously, wherein the particular software processes and reproduces relatively small data packets sequentially. If, for example, a stereophonic audio signal represents the multimedia data quantity, splitting can take place in such manner that only the stereo component (difference of right and left channel) is moved into the essence file. The basic file subsequently contains the monophonic audio signal such that for a high quality stereo reproduction the essence file is necessary. If the data quantity is a video file, then, for example every 10 seconds, complete frames could be moved into the essence file. If for the processing of video data, delta compression methods are utilized, in which always only the difference from the preceding frame is stored, it is better to move the first frame after a scene change into the essence file.

[0036] In general, care should be taken that in the division of the multimedia data quantity no redundant data are moved into the essence file, since these can readily be reproduced in the basic file without the essence file being required for this purpose. With certain file types it can therefore be useful to carry out the splitting of the data quantity only after a suitable compression by which the redundant data are largely removed.

[0037] Fig. 2 shows in a block diagram the principle of the processing of multimedia data quantities which are present after the split into the basic file 6 and the essence file 7. The depicted example is of the "dynamic" data type, which is also denoted as streaming data. The multimedia data quantity comprises, for example, 100 data packets. From the total data quantity in the depicted case ten data packets are removed and transferred into the essence file 7. The basic file 6 therewith lacks significant data distributed (more or less uniformly) over the data quantity, which data are required for the reproduction of the multimedia data quantity at a high level of quality.

[0038] When combining the basic file 6 and the essence file 7 on the local computer, decryption of the data packets of the essence file 7 takes place in a decryption unit 11 since the essence file 7 is available only in its encrypted state on the local computer (see below). In a mixer 12 subsequently the individual data packets from the basic file 6 and the essence file 7 are joined in the correct sequence. The mixer 11 must therefore be informed of the rule for the combination of the data. The data packets, which are subsequently again in the correct sequence, are supplied in conventional manner to a decoder 13 which generates a multimedia output signal

and conducts it to an output apparatus 14.

[0039] The manner in which the basic file and the essence file are combined depends on the utilized data types and the method applied for the data division. Therefore to the application program executing on the local computer information must be conveyed regarding the algorithm to be used for combining the basic file and the essence file. Details in this regard will be explained below.

[0040] Figure 3 shows a flow chart, in which individual steps are depicted which are carried out before or during the transmission of an essence file from a server to a local computer. As was already explained earlier, on the local computer a data processing program is executed which requires a multimedia data quantity. If the data processing program is to execute a particular function, by querying a local system registration data base determination is made of whether or not the required essence file 7 is available on the local computer which is required for the supplementation of the basic file 6. The system registration data base is provided under the operating system Windows by the so-called Registry (RG). The Registry contains also entries, based on which the application program can determine whether or not the particular user wishes to access the required essence file for the first time, whether or not a repeat access takes place or whether or not other essence files are already available on the local computer for the same data processing program.

[0041] With respect to Fig. 3, first, the case is considered that the data processing program accesses a function for the first time, which function requires a specific essence file. This case is referred to here as new registration, the user of the local computer being a new customer. The procedure starts in step 20. The user receives in step 21 the comment that the required essence file is not available on the local computer and that therefore an online connection with a pay-per-use server can be established in order to obtain the essence file from this server.

[0042] The pay-per-use server is a computer with a permanent connection to the Internet. The software running on this server is comparable to a so-called e-commerce shop. The server has a data interface to the connected data network, in the discussed example, thus to the World Wide Web. The server, however, is especially configured in so far that it can only be addressed by a special pay-per-use client. As was explained above, the pay-per-use client is realized on the local

computer. The restriction of the access capabilities to the server increases the security, since any other computers cannot readily access this server. This specially set-up server is denoted in Fig. 3 by the label "4fo".

[0043] When a user decides in step 21 to establish a connection with the server, the necessary connection to 4fo is established in step 22 and the initial data transmission can start. However, the local computer could also be so configured that no intervention by the user is required, but rather the particular required essence file is automatically loaded from the server, if necessary. To this end, the client transmits special parameters to the server using the so-called POST method. These parameters are required in order to inform the server as to which information (essence file) is required.

[0044] To determine the identity of the user or of the local computer, the transmitted parameters are additionally provided with a digital signature. For this purpose, ahead of time, for example by application of an asymmetric encryption method, a key pair is formed, The public part of the key pair (public key) is transmitted to the server. If, as was explained with respect to Fig 1, a smart card is used, the public key can be read from the smart card.

[0045] In order to make authorization of the server with respect to the client possible, a second key pair is utilized. This second key pair is application specific. The private key remains on the server. The public key is a component of the client. If the data transmitted from the server utilizing the private key are signed, then the local computer can check whether or not the received data originate, in fact, from the dialed server such that data manipulation by third parties is excluded.

[0046] In step 23 the server checks the signature of the user who registers for the first time. If in step 24 it is determined that the parameters were transmitted free of falsification from the new user, in step 25 the registration of the new customer starts. To this end a login (username) is defined for the new customer.

[0047] Fig. 4 shows the general structure of a feasible form page, which is utilized during the registration of a user at the server. This form page has a constant menu bar and a variable portion. It is understood that in the case of modified implementations, a different structure can also be selected.

[0048] Back to Fig. 3. Here the form page according to Fig. 4 is depicted in individual method steps, wherein certain control fields are blanked out if the associated actions are not available at the specific site in the procedure. To check the data of the user, in step 26 the message regarding the login and in particular of the password can be sent per e-mail to the user.
This ensures at least that the e-mail address of the user is correct. After in step 27 the data check was confirmed as successful, in step 28 an initialization password and a customer number is determined. The password is, for example, a 64-bit number, which was base64 encoded. The encoded password and the customer number are sent by e-mail in step 29 to the user. If the user so wishes, the password can be stored locally or entered each time when executing the data processing program. The customer number is used if payment for receipt of the essence file must be made and these payments are to be triggered through instruction per telephone.
[0049] Subsequently, on the server in step 30 a transfer archive is generated which contains the essence file in encrypted form. The essence file is preferably encrypted each time with a unique session-specific key (session key) just before the integration into the transfer archive. The special structure of the transfer archive will be explained below. In step 31 the created transfer archive is transmitted to the local computer. For this purpose a special component is utilized, which makes it possible to accept the transfer archive and to transfer it into the main store of the local computer. As soon as the transfer archive is available on the local computer, it is checked for integrity and correct digital signature and can subsequently be stored on a local data medium. When creating the transfer archive on the server, a unique session characteristic can be generated and saved in the transfer archive, from which a unique file name can be generated for storage on the local computer. To this end, for example, the time of generation of the transfer archive can be utilized. The transfer archive contains, furthermore, the above described session key in encrypted form.
[0050] Lastly, in step 32 the installation of the transfer archive at the user end takes place, in which *inter alia* the transfer archive and the essence files contained therein are registered in the system registration data base. Therewith it is also possible, with a repeated transmission of certain essence files (for example in the event of an update) to update the memory location of the particular essence files in the registration data base such that the data processing program

accesses the most up-to-date version of the individual essence files. The procedure could end at this point since the essence file has been installed on the local computer and is usable to the authorized user. However, the procedure can also be continued as is evident in Fig. 3. The succeeding method steps will be explained below.

[0051] Fig. 5 shows the general structure of a transfer archive, such as was created on the server. The transfer archive in general is comprised of one or several essence files (plugins), an archive header, a digital signal (server signature) provided by the server and a check sum (Crc32). Before integrating the essence file into the transfer archive, this file is encrypted utilizing a symmetric encryption method. The symmetric key forms, for example a 128-bit number, which is randomly determined as a session key on the server for each individual session or by request of a user. This session key is furthermore asymmetrically encrypted with the public key of the particular user and subsequently also stored in the transfer archive. Decryption of the essence file 7 can thus only take place if the private key of the user is available, which is stored, for example, on the smart card. The check sum Crc32, which is also integrated in the transfer archive, can be utilized in order to check whether or not the decryption was performed correctly. A further increase of the security is attained thereby that the private key of the key registered at the server is additionally symmetrically encrypted with the assigned password, which can be sent per e-mail to the user to check the user's identity.

[0052] In an embodiment reduced to practice, the following known algorithms for encryption can be applied:

Asymmetric method: RSA 1024 bit

Symmetric method: Blowfish 128 bit (Safer, Square)

Password: 64-bit random number recoded with base64.

Hash function (for digital signature): SHA1.

[0053] The data processing program running on the local computer during the access to the particular essence file calls up the encryption routine such that the decryption is carried out in real time and the essence file is only available in the encrypted state on the permanent data medium of the local computer. If indicated, the essence file can be compressed loss-free before the encryption, which requires decompression during the execution of the data processing

program on the local computer.

[0054] When the user at a renewed execution of the data processing program calls up a function which requires the essence file 7, the data processing programs by accessing the system registration data base determines that the essence file is already available on the local computer. From the registration data base that transfer archive can be determined in which the essence file is contained. For the case that several essence files are stored in a common transfer archive, the registration data base also contains an entry regarding the position of the particular essence file in the transfer archive. In that case, no renewed request for the essence file from the server is required.

[0055] In the archive header the transfer archive also contains specifications regarding the routine to be executed with which the basic file and the essence files are to be linked. In the transfer archive is also contained the particular session key for the individual essence files, which must be decrypted using the private key of the user. Since the essence file itself had been encrypted with a symmetric encryption method, the decryption can take place during the execution of the data procession program (on the fly), since in the case of symmetric encryption methods a sufficiently fast decryption can be carried out as soon as the symmetric key has been decrypted.

[0056] It should also be emphasized that on the server are also stored the user-specific data. These permit at a later access by the user to the server the immediate identification of the user as well as the check of the essence files already sent to this user. Thereby can be ensured that the user does not need to obtain twice certain essence files from the server. Even if through a data loss the essence files stored at the user end are damaged, in this way a renewed download from the server can be enabled without the already paid for essence files needing to be paid by the user again. In addition, the server can also manage information regarding a user account from which an appropriate amount can be debited when the user purchases essence files. The server, moreover, also keeps all essence files (plugins) available for a certain application in unencrypted form, which are packaged in encrypted form and in a user-specific transfer archive when the user wishes to purchase these essence files.

[0057] In Fig. 3 furthermore is depicted the procedure if the user no longer has available the

private key which is required for the decryption of the essence files. This case can occur, for example, if the private key is not stored on a smart card but rather was determined with respect to certain hardware components of the local computer and a change of the hardware components has taken place. The communication necessary in this case between the local computer is started in step 40. If in step 41 it was determined that a connection with the server is being established, a new key pair is created and in step 42 again the connection to the server is established. Herein the new public key is transmitted. In step 43 the new private key of the user/local computer is checked. If the check was successful in step 44, the server switches in step 45 into a repeat registration dialog, wherein the user name (login) is unchangeable. In step 46 the server carries out a password check. The password is known to the user from the e-mail sent by the server. If the password is confirmed in step 47, a new password can be determined in step 48. The procedure is subsequently continued with step 29, so that the user can receive further essence files from the server.

[0058] The private key can be either stored on the smart card or be stored in encrypted and/or concealed form on the local data medium of the local computer.

[0059] For this purpose it is suitable, for example, tying the private key to special hardware characteristics of the local computer.

[0060] The renewed registration can also be required if the user of the data processing program has newly installed his computer. To this end, the user can branch into a repeat registration dialog (step 50). After he has entered his old login, the login and the password are checked in step 51. Following confirmation in step 52, in step 48 a new password can be determined. The procedure is subsequently continued as described in step 29.

[0061] Lastly, in Fig. 3 the necessary procedure is shown for the case in which a user or local computer, already known to the server, requires a further essence file, for example in order to execute in the data processing program to be executed locally an additional level of a computer game. The reregistration of the user for transmission of a further essence file starts in step 60. Before 60 a decision is made again of whether or not the required essence file is to be obtained from the server. After a callback in step 61, a connection is established with the server in step 62. The pay-per-use client transmits using the POST method the parameters required for the

connection, in particular the user name (login), identification data for the data processing program, identification data for the required essence file and a digital signature. The signature is checked in step 63. If the transmitted data could be verified in step 64, the user immediately gains access to the selection area (e-shop), where he can select further essence files (plugins) for downloading (step 65). In a modified embodiment, this step can be omitted if through the first data transmission it had already been determined which essence file is required and therewith a further selection is not required.

[0062] In step 66 an individual transfer archive is created which contains the requested essence files. In step 67 the transfer archive is transmitted to the local computer, such that here in step 68 in the described manner the transfer archive can be checked and stored.

[0063] If a user known per se to the server wishes to purchase essence files for another data processing program (for example a new computer game), he can be treated at the server as an old user, to whom, for this new data processing program, a new password is assigned such that the corresponding procedure starting in step 20 is followed.

[0064] The described method for the distribution of multimedia data quantities and the data processing system can also be utilized for other multimedia data quantities. It would be conceivable, for example, to shift certain detail information from electronic maps into these essence files which the user can only obtain when needed.

Patent Claims

1. Method for making available multimedia data quantities for a user, comprising the following steps:

- providing an essence file (7) on a remote server (3), which file comprises at least a portion of the multimedia data quantity;
- encrypting the essence file;
- transmitting the encrypted essence file to a local computer (1) to which the user has access;
- storing the encrypted essence file on a local data medium of the local computer;
- decrypting the essence file during the execution of a data processing program (2) on the local computer;
- reproducing the multimedia data quantity via an output apparatus during the execution of the data processing program on the local computer.

2. Method as claimed in claim 1, wherein the essence file (7) comprises the complete multimedia data quantity.

3. Method as claimed in claim 1, wherein the essence file does not comprise the entire multimedia data quantity, comprising the following steps:

- division of the multimedia data quantity into a basic file (6) and an essence file (7), according to a predetermined division algorithm;
- transmission of the basic file and of the essence file;
- joint storage of the basic file and of the encrypted essence file on a local data medium of a local computer (1);
- linkage of the basic file and of the essence file to form the multimedia data quantity during the execution of the data processing program (2) on the local computer, after the decryption of the essence file.

4. Method as claimed in claim 3, wherein the step of division of the data quantity comprises the extraction of significant portions of the data quantity into the essence file, such that the basic file without the essence file can no longer be reproduced on the output apparatus or only at reduced quality or reduced extent of functions.

5. Method as claimed in claim 4, wherein from the data quantity at least portions of the file header information (header), which is necessary for the interpretation of the remaining data, is extracted and integrated into the essence file.

6. Method as claimed in claim 4, wherein before their coding stereophonic audio data are divided into a monophonic data stream (sum signal: right plus left channel) and a difference data stream (right minus left channel), and wherein the right-left data stream forms the essence file.

7. Method as claimed in claim 4, wherein the data shifted into the essence file are only extracted from the compressed data quantity after a compression of the multimedia data quantity.

8. Method as claimed in one of claims 1 to 7, wherein the encryption of the essence file takes place using a symmetric encryption algorithm, and wherein the session-specific key (session key) utilized for this purpose, in turn, is encrypted using an asymmetric encryption algorithm.

9. Method as claimed in claim 8, comprising furthermore the following steps:

- determination of a random number as the session-specific key (session key);
- encryption of the essence file (7) with the session-specific key using the symmetric encryption algorithm;
- encryption of the session-specific key with the public key of a key pair belonging to the user, using the asymmetric encryption algorithm;
- repeat encryption of the asymmetrically encrypted session key with a user-specific key (password) using a symmetric encryption algorithm.

10. Method as claimed in claim 9, wherein the step of transmission of the encrypted essence file comprises the generation of a transfer archive which is transmitted and which comprises the following components:

- the encrypted essence file;
- a server signature which permits the identification of the remote server;
- a check section which permits an error check of the transfer archive;
- a data identification section;
- a user data section which permits the identification of the user;
- the encrypted session key for the decryption of the essence file.

11. Method as claimed in one of claims 1 to 10, wherein, after the storage of the encrypted essence file on the data medium of the local computer, entries in a system registration data base of the local computer are generated, from which the data processing program during the execution can be determine the storage position of the essence file.

12. Method as claimed in claim 9 in so far as it refers back to claim 3, wherein the transfer archive with the encrypted essence file is transmitted via an online connection from the server to the local computer, and wherein furthermore the following steps are performed:

- transmission of a request for the essence file from the local computer to the server;
- check of the authorization of the user to receive the essence file;
- generation of the transfer archive on the server;
- execution of a finance transaction for payment of the essence file, before the transfer archive is transmitted to the local computer.

13. Method as claimed in one of claims 1 to 12, wherein on the server data are stored which permit the unique identification of the local computer, of the essence files transmitted to this [local computer], and optionally of the particular user.

14. Data processing system for making available multimedia data quantities comprising:

- a remote server (3) with a server data medium;
- a local computer (1) with a local data medium and an output apparatus (14) for multimedia data, which computer executes a data processing program utilizing the multimedia data;
- an at least temporary data transmission connection (4) between the server and the local computer,

characterized by

- an encryption unit encrypting an essence file, which comprises at least a portion of the multimedia data quantity;
- an archive generation unit of the server, which combines the encrypted essence file with user-specific data to form a transfer archive and makes this [archive] available for online transmission via the data transmission connection;
- an updating unit of the local computer, which carries out entries into a system registration data base of the local computer, which [entries] indicate the contents of the transmitted transfer archive;
- a decryption unit of the local computer which, during the execution of a data processing program (2), decrypts the essence file; and
- an output unit which outputs the multimedia data quantity to the output apparatus.

15. Data processing system as claimed in claim 14, furthermore characterized by

- a file division unit, which divides the multimedia data quantity into a basic file (6) and an essence file (7); and
- a combination unit of the local computer, which links the decrypted essence file according to a combination algorithm with the basic file to form the multimedia data quantity.

16. Data processing system as claimed in claim 14 or 15, characterized in that

- the encryption unit encrypts the essence file (7) with a session-specific key (session key) through a symmetric encryption algorithm;
- the archive generation unit encrypts the session-specific key with the public key of a key pair of the user encrypted using an asymmetric encryption algorithm and adds it to the transfer archive;
- the decryption unit with the aid of the private key of the key pair of the user decrypts the session-specific key and with it decrypts the essence file.

17. Data processing system as claimed in claim 16, characterized in that the archive generation unit furthermore encrypts the session-specific key (session key) with a user-specific key (password) using a symmetric encryption algorithm.

18. Data processing system as claimed in claim 16 or 17, characterized in that the private key of the user is stored in encrypted form on the local computer, wherein the private key using a symmetric encryption method is encrypted with a user-specific key and wherein the user-specific key is generated according to a predetermined generation algorithm from technical device characteristics (hardware) and the configuration characteristics of the local computer.

19. Data processing system as claimed in claim 16 or 17, characterized in that the local computer comprises a smart card unit with a smart card, on which the private key of the user is stored, wherein the decryption unit accesses the smart card for the decryption of the symmetric key.

20. Data processing system as claimed in one of claims 14 to 19, characterized in that the individual units are realized through software routines.

21. Computer configured as server and capable of establishing a data transmission connection to another computer, comprising:

- a file division unit which divides a multimedia data quantity into a basic file and an essence file;
- an encryption unit, which encrypts the essence file;
- an archive generation unit which combines the encrypted essence file with specific data of a connected computer to form a transfer archive and makes this [file] available for the online transmission via the data transmission connection;
- a user data base in which user-specific data, including the characteristics of the transmitted transfer archive, are stored.

22. Computer as claimed in claim 21, characterized in that furthermore a key generation unit is provided, which generates a random session-specific key (session key) for the encryption of the essence file.

23. Computer configured as a local computer, capable of establishing a data transmission connection to a server, wherein it assumes the function of client, and comprises an updating unit and comprises an updating unit, which carries out entries into a system registration data base specifying the contents of a transfer archive transmitted from the server, wherein on the local computer a data procession program can be executed which, during its execution, decrypts an essence file contained in the transfer archive, links the decrypted essence file according to a combination algorithm contained in the transfer archive with a locally stored basic file to form a multimedia data quantity and outputs it to an output apparatus.

---

5 drawing sheets enclosed

Fig. 1

2 Application with pay-per-use client
4 Request
6 Basic file
7 Essence file

Fig. 2

6 Basic file 90 packets
7 Essence file 10 packets
14 Output
11 Decryption

Fig. 3

60 Repeat login - download
20 New login - new customer
40 Private key lost - new key
61 Online comment - do you want to connect to 4fo
21 Online comment - do you want to connect to 4fo?
41 Online comment - do you want to connect to 4fo?
62 Connection with 4fo transmission of data (without public key)
22 Connection with 4fo transmission of data (with public key)
42 Connection with 4fo transmission of data (with public key)
63 Download signature check
23 Newcustomer signature check
43 Newkey signature check
65 Plugin selection
25 Registration with login determination
26 Data check (for example e-mail)
50 Repeat registration dialog (name var.)
51 Login/password check
45 Repeat registration dialog (name fixed)
46 Password check
28 Determine password, customer number
48 Determine new password
29 E-mail with password, login, customer number
66 Create archive with plugins
67 Download archive
68 Check archive and store
30 Create archive with user data
31 Download archive
32 Install user

Fig. 4

From left to right:
Login - back - OK - user data - help

right hand side: Constant menu bar
Variable portion of page

Fig. 5

Line:
<archiveVersion> :: = 32 bit integer (unsigned) 0x2 = current structure

<archiveID> :: = 32 bit integer (unsigned)
uniquely describes archive (with version)
protocols continuously the archive output for a GameID

<createDate> :: = 8 Bytes
creation data, format: for example 01202000 for 20 January 2000

<customerNo> :: = 32 bit integer (unsigned) customer number
<customernName> :: = 33 Bytes (= max. 32 characters + remainder #0)
login name/nickname (Ansi character set, letters
(international) and [0-9]_. -<blank>)

<encipheredKey> :: = 172 Bytes (base64 coding)
128 bit random number = symmetric key
can be increased later, with password (64bit symmetric)
and the public key (1064 asymmetric) of customer encrypted

<nmbPlugins> :: = 32 bit integer (unsigned) denotes the length of the filename

<pluginData> ::
(Blowfish encryption)

<pluginRawData> :: =
Plugin (together with remaining file yields original file)

<paddingBytes> :: = Random Bytes
Increase to next 8 Bytes window by **<pluginData>**

Strings are stored in fields of constant length. Non-occupied characters are filled with binary zeroes.

4FOArchive Filename:

The file name of the transfer archive is derived directly from the SessionID of the pay-per-use server: <last 32 characters of the sessionID>.4fo